

AMENDMENTS TO THE CLAIMS:

This listing of claims will replace all prior versions and listings of claims in the application:

1. (Currently Amended) An information recording apparatus comprising:
inputting means for inputting enciphered contents information;
contents information deciphering means for deciphering the enciphered contents information;

access position extracting means for extracting recording medium access positions from the deciphered contents information, the recording medium access positions indicating addresses on a recording medium corresponding to a time stamp in the contents information;

management information creating means for creating management information that includes the recording medium access positions from the deciphered contents information; and

recording means for recording the enciphered contents information on a first area of a recording medium, recording information for enciphering the contents information on a second area of the recording medium, and recording the management information on a third area of the recording medium.

2. (Canceled)

3. (Original) The information recording apparatus according to claim 2 wherein said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems, and wherein

said management information shows the access positions for said contents information by means of the time stamps for said transport streams and addresses on the recording medium.

4. (Original) The information recording apparatus according to claim 1 wherein, as access positions described in the management information, positions where random accesses are possible to said contents information are extracted.

5. (Original) The information recording apparatus according to claim 4 wherein said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

6. (Currently Amended) An information reproducing apparatus comprising:
reading means for reading contents information and management information from a recording medium, the management information including recording medium access positions that indicate addresses on the recording medium corresponding to a time stamp in the contents information; and

reading position controlling means for controlling the reading positions of the contents information on the recording medium based on the management information read from the recording medium;

wherein the contents information is enciphered; and

wherein the ~~management information includes~~ recording medium access positions are determined from the contents information ~~previously extracted from the deciphered contents information.~~

7. (Original) The information reproducing apparatus according to claim 6 wherein said management information shows the access positions for the contents information by means of time information of the contents information and addresses on the recording medium.

8. (Original) The information reproducing apparatus according to claim 7 wherein said contents information is recorded on the recording medium in the form of transport streams prescribed by the MPEG 2 systems; and

said management information shows the access positions for said contents information by means of the time stamps of said transport stream and addresses on the recording medium.

9. (Original) The information reproducing apparatus according to claim 6 wherein, as access positions described in said management information, positions where random accesses to said contents information are available are shown.

10. (Original) The information reproducing apparatus according to claim 9 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

as access positions described in said management information, transport packets each containing a sequence header code are shown.

11. (Currently Amended) An information recording/reproducing apparatus comprising:

inputting means for inputting enciphered contents information;

contents information deciphering means for deciphering the enciphered contents information;

access position extracting means for extracting recording medium access positions from the deciphered contents information, the recording medium access positions indicating addresses on a recording medium corresponding to a time stamp in the contents information;

management information creating means for creating management information that includes the recording medium access positions from the deciphered contents information;

recording means for recording the enciphered contents information on a first area of a recording medium, recording information for enciphering the contents information on a second area of the recording medium, and recording the management information on a third area of the recording medium.

reading means for reading the contents information and the management information from the recording medium; and

reading position controlling means for controlling the reading positions of the contents information on the recording medium based on the management information read from the recording medium.

12. (Canceled)

13. (Original) The information recording/reproducing apparatus according to claim 12 wherein said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and addresses on the recording medium.

14. (Original) The information recording/reproducing apparatus according to claim 11 wherein, as access positions described in said management information, positions where random accesses for said contents information are possible are extracted.

15. (Original) The information recording/reproducing apparatus according to claim 14 wherein said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and wherein

for the access positions described in said management information, transport packets each containing a sequence header code are extracted.

16. (Currently Amended) An information recording method comprising the steps of:

inputting enciphered contents information;

deciphering the contents information;

extracting recording medium access positions from the deciphered contents information, the recording medium access positions indicating addresses on a recording medium corresponding to a time stamp in the contents information;

creating management information that includes the recording medium access positions from the deciphered contents information; and

recording the enciphered contents information on a first area of a recording medium, recording information for enciphering the contents information on a second area of the recording medium, and recording the management information on a third area of the recording medium.

17. (Canceled)

18. (Original) The information recording method according to claim 17 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps for said transport stream and the addresses on the recording medium.

19. (Original) The information recording method according to claim 16 wherein, as access positions described in said management information, positions where random accesses are possible for said contents information are extracted.

20. (Original) The information recording method according to claim 19 wherein, said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and

as access positions described in said management information, transport packets each containing a sequence header code are extracted.

21. (Currently Amended) An information reproducing method comprising the steps of:

reading contents information and management information from a recording medium, the management information including recording medium access positions that indicate addresses on the recording medium corresponding to a time stamp in the contents information; and

controlling the reading positions of the contents information on the recording medium based on the management information read from the recording medium;

wherein the contents information is enciphered; and

wherein the ~~management information includes~~ recording medium access positions are determined from the contents information ~~previously extracted from the deciphered contents information.~~

22. (Canceled)

23. (Original) The information reproducing method according to claim 22 wherein, said contents information is recorded on a recording medium in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport streams and the addresses on the recording medium.

24. (Original) The information reproducing method according to claim 21 wherein, as access positions described in said management information, positions where random accesses to said contents information are possible are shown.

25. (Original) The information reproducing method according to claim 24 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and

as access positions described in said management information, transport packets each containing a sequence header code are indicated.

26. (Currently Amended) An information recording/reproducing method comprising the steps of:

during the recording process:

inputting enciphered contents information;

deciphering the contents information;

extracting recording medium access positions from the deciphered contents information, the recording medium access positions indicating addresses on a recording medium corresponding to a time stamp in the contents information;

creating management information that includes the recording medium access positions from the deciphered contents information; and

recording the enciphered contents information on a first area of a recording medium, recording information for enciphering the contents information on a second area of the recording medium, and recording the management information on a third area of the recording medium.

during the reproducing process:

reading the contents information and the management information from the recording medium; and

controlling the reading positions of the contents information on the recording medium based on the management information read from the recording medium;

wherein the contents information is enciphered; and

wherein the ~~management information includes~~ recording medium access positions are determined from the contents information ~~previously extracted from the deciphered contents information.~~

27. (Canceled)

28. (Original) The information recording/reproducing method according to claim 27 wherein, said contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

said management information shows the access positions for said contents information by means of the time stamps of said transport stream and the addresses on the recording medium.

29. (Original) The information recording/reproducing method according to claim 26 wherein, as access positions described in said management information, positions where random accesses to said contents information are possible are extracted.

30. (Original) The information recording/reproducing method according to claim 29 wherein, said contents information is inputted in the form of the transport streams prescribed by the MPEG 2 systems; and

as access positions described in said management information, transport packets each containing a sequence header code are extracted.

31. (Currently Amended) A recording medium wherein the following are recorded:

enciphered contents information, and
processor readable management information that includes instructions for causing the processor to access process data stored at recording medium access positions on the recording medium, the recording medium access positions indicating addresses on the recording medium corresponding to a time stamp in the contents information.

32. (Canceled)

33. (Currently Amended) The information recording apparatus according to claim 1 further comprising:

receiving means for receiving, from another device, enciphered contents information and a contents key ~~cipher keys~~ used to encipher the contents information ~~transmitted from other apparatuses by means of communication means~~; and

~~cipher contents key~~ enciphering means for enciphering the contents key using a medium key; ~~creating enciphered cipher keys obtained by enciphering cipher keys received by the receiving means by the first cipher key, and~~

wherein the contents information deciphering means deciphers the enciphered contents information received from the other device ~~uses the received cipher key to decipher the enciphered contents information received to obtain contents information~~; and

wherein the recording means records the enciphered contents key ~~cipher keys~~ on the recording medium as the information for enciphering the contents information.

34. (Currently Amended) The information recording apparatus according to claim [[1]] 33 further comprising:

~~first cipher medium~~ key creating means for choosing the ~~first cipher medium~~ key used to encipher the ~~cipher contents~~ key by using a formula that includes recording medium identification information read from the recording medium.

35. (Currently Amended) The information recording apparatus according to claim [[1]] 33 further comprising:

~~first cipher medium~~ key creating means for choosing the medium ~~the first cipher~~ key used to encipher the ~~cipher contents~~ key; and

~~second cipher master~~ key creating means for choosing a master ~~the second-~~
cipher key used to encipher the ~~first cipher~~ medium key by using a formula that includes
the recording medium identification information read from the recording medium.

36. (Currently Amended) The information recording apparatus according to claim
[[1]] 33 further comprising:

~~second cipher master~~ key creating means for choosing a master ~~the second-~~
cipher key; the master key used to encipher the medium key and chosen using a
formula that includes recording medium identification information read from the
recording medium; ~~used to decipher the first cipher key enciphered and read from the~~
~~recording medium based on the recording medium identification information read from~~
~~the recording medium;~~ and

~~first cipher~~ medium key deciphering means for deciphering the medium key
enciphered by the master key; ~~the first cipher key enciphered by using the second-~~
~~cipher key created,~~

wherein the ~~cipher~~ contents key enciphering means enciphers the ~~cipher keys~~
contents key received from the receiving means by using the ~~first cipher~~ medium key.

37. (Currently Amended) The information recording apparatus according to claim
1 further comprising:

receiving means for receiving, from another device, enciphered contents
information and ~~the cipher keys~~ a contents key used to encipher the contents
information ~~transmitted from other apparatuses by means of communication means;~~

~~cipher key creating~~ information creating means for creating ~~cipher key creating~~
contents key generation information that can be used to create generate the contents
key ~~cipher keys based on the cipher keys received from by~~ the receiving means; and

~~cipher key creating~~ contents key generation information enciphering creating
means for enciphering the contents key generation ~~creating enciphered cipher key-~~
~~creating~~ information with a medium key ~~obtained by enciphering by the first cipher key-~~
~~the cipher key creating information created, and~~

wherein the contents information deciphering means deciphers the enciphered
contents information ~~received by means of cipher keys received to restore contents-~~
information; and

wherein the recording means records the enciphered ~~cipher key creating~~
contents key generation information on the recording medium as the information for
enciphering the contents information.

38. (Currently Amended) The information recording apparatus according to claim
[[1]] 33 wherein, the management information shows the access positions for contents
information by means of the time information for contents information and the addresses
on the recording medium.

39. (Currently Amended) The information recording apparatus according to claim
[[1]] 38 wherein, the contents information is inputted in the form of transport streams
prescribed by the MPEG 2 systems; and

the management information shows the access positions for the contents
information by means of the time stamps of the transport streams and the addresses on
the recording medium.

40. (Currently Amended) The information recording apparatus according to claim [[1]] 33 wherein, as access positions described in the management information, positions where random accesses for the contents information are possible are extracted.

41. (Currently Amended) The information recording apparatus according to claim [[1]] 40 wherein,

the contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and

for the access positions described in the management information, transport packets each containing a sequence header code are extracted.

42. (Canceled)

43. (Currently Amended) The information ~~recording~~ reproducing apparatus according to claim 6 wherein: [[,]]

the recording medium contains an enciphered ~~cipher~~ contents key,

the contents key is the key used to encipher the contents information, obtained by enciphering the cipher key used for enciphering contents information as information for enciphering the contents information, and further comprising:

the information reproducing apparatus further comprising cipher key a contents key deciphering means for deciphering the contents key enciphered cipher key using a medium key by means of the first cipher key.

44. (Currently Amended) The information reproducing apparatus according to claim [[6]] 43 further comprising:

~~first cipher medium~~ key creating means for choosing the ~~first cipher medium~~ key used to decipher the ~~cipher contents~~ key, ~~by the cipher key deciphering means the medium key chosen~~ using a formula that includes the recording medium identification information read from the recording medium.

45. (Currently Amended) The information reproducing apparatus according to claim [[6]] 43 further comprising:

~~first cipher medium~~ key deciphering means for deciphering the ~~first cipher medium~~ key used to decipher the ~~cipher key~~ using the ~~second cipher~~ a master key; and ~~second cipher master~~ key creating means for choosing the ~~second cipher master~~ key, the master key chosen using a formula that includes ~~used to decipher the first cipher key by means of~~ the recording medium identification information read from the recording medium.

46. (Currently Amended) The information reproducing apparatus according to claim [[6]] 43 further comprising:

~~second cipher master~~ key creating means for choosing the ~~second cipher~~ a master key used to decipher the ~~first enciphered cipher medium~~ key read from the recording medium, the master key chosen using a formula that includes ~~based on the recording medium identification information read from the recording medium; and~~ ~~first cipher medium~~ key deciphering means for deciphering the ~~first cipher medium~~ key ~~enciphered by means of the second cipher key created.~~

47. (Currently Amended) The information reproducing apparatus according to claim 6 wherein, the recording medium contains ~~enciphered cipher key creating information~~ enciphered contents key generation information ~~obtained by enciphering the~~

~~cipher key creating information for creating the cipher keys used to encipher the contents information; and further comprising:~~

~~cipher key creating~~ contents key generation information deciphering means for deciphering the ~~enciphered cipher key creating~~ contents key generation information by means of the first cipher using a medium key; and

~~cipher key creating~~ contents key generating means for generating a contents key using the contents key generation information ~~creating the cipher key based on the cipher key creating information deciphered by the first cipher key.~~

48. (Currently Amended) The information reproducing apparatus according to claim ~~[[6]]~~ 43 wherein, the management information shows the access positions for contents information by means of the time information of the contents information and the addresses on the recording medium.

49. (Currently Amended) The information reproducing apparatus according to claim ~~[[6]]~~ 48 wherein, the contents information is inputted by transport streams prescribed by the MPEG 2 systems; and

the management information shows the access positions for the contents information by means of the time stamps of the transport streams and the addresses on the recording medium.

50. (Currently Amended) The information reproducing apparatus according to claim ~~[[6]]~~ 43 wherein, as access positions described in the management information, positions where random accesses are possible for the contents information are extracted.

51. (Currently Amended) The information reproducing apparatus according to claim ~~[[6]]~~ 50 wherein, the contents information is inputted by transport streams prescribed by the MPEG 2 systems; and wherein

for access positions described in the management information, transport packets each containing a sequence header code are extracted.

52. (Canceled)

53. (Currently Amended) The information recording/reproducing apparatus according to claim 11 further comprising:

receiving means for receiving, from another device, enciphered contents information and a contents key ~~the cipher keys~~ used to encipher the contents information ~~transmitted from other apparatuses by means of communication means;~~
and

~~cipher~~ contents key enciphering means for enciphering the contents key ~~creating enciphered cipher keys obtained by enciphering the cipher keys by means of the first cipher key;~~ and

~~cipher~~ contents key deciphering means for deciphering the ~~enciphered cipher keys~~ contents key by means of a medium ~~the first cipher key~~, and

wherein the contents information deciphering means deciphers the ~~enciphered contents information~~ received from the other device ~~received by means of the cipher keys received to obtain contents information;~~ and

wherein the recording means records the enciphered contents key ~~cipher keys~~ on the recording medium as the information for enciphering the contents information.

54. (Currently Amended) The information recording/reproducing apparatus according to claim 44 53 further comprising:

~~first cipher~~ medium key creating means for choosing ~~the first cipher~~ the medium key used to encipher the ~~cipher keys~~ contents key by using a formula that includes ~~means of the~~ recording medium identification information read from the recording medium.

55. (Currently Amended) The information recording/reproducing apparatus according to claim 44 53 further comprising:

~~first cipher~~ medium key creating means for choosing the ~~first cipher~~ medium key used to encipher the ~~cipher keys~~ contents key;

~~first cipher~~ medium key deciphering means for deciphering the ~~first cipher~~ medium key used to decipher the ~~cipher keys~~ by means of the ~~second cipher~~ using a master key; and

~~second cipher~~ master key creating means for choosing the ~~second cipher~~ master key used to encipher the medium ~~first cipher~~ key, the master key created by means of ~~the~~ using a formula that includes recording medium identification information read from the recording medium.

56. (Currently Amended) The information recording/reproducing apparatus according to claim 44 53 further comprising:

~~second cipher~~ master key creating means for choosing a master ~~the second~~ ~~cipher key, the master key used for deciphering the medium key and chosen using a~~ formula that includes recording medium identification information read from the recording medium ~~for deciphering the first cipher key enciphered and read from the~~

~~recording medium based on the recording medium identification information read from the recording medium; and~~

~~first cipher medium key deciphering means for deciphering the medium key using the master key enciphered by means of the second cipher key created, and~~

~~wherein the cipher contents key enciphering deciphering means deciphers the cipher keys contents key received by the receiving means using the medium key by means of the first cipher key.~~

57. (Currently Amended) The information recording/reproducing apparatus according to claim 11 further comprising:

~~receiving means for receiving, from another device, enciphered contents information and the cipher keys a contents key used to encipher the contents information transmitted from other apparatuses by communication means;~~

~~cipher key creating information creating means for creating contents key generation information cipher key creating information that can be used to generate the contents key create such cipher keys; and~~

~~cipher key creating contents key generation information enciphering means for creating enciphered cipher key creating enciphering the contents key generation information with the medium key obtained by enciphering the cipher key creating information created by the first cipher key, and~~

~~wherein the contents information deciphering means deciphers the enciphered contents information received by means of the cipher key received to restore contents information; and~~

wherein the recording means records the enciphered ~~cipher key creating~~
contents key generation information on the recording medium as the information for
enciphering the contents information.

58. (Currently Amended) The information recording/reproducing apparatus
according to claim 44 53 wherein, the management information shows the access
positions for contents information by means of the time information for contents
information and the addresses on the recording medium.

59. (Currently Amended) The information recording/reproducing apparatus
according to claim 44 58 wherein, the contents information is inputted in the form of
transport streams prescribed by the MPEG 2 systems; and wherein

the management information shows the access positions for the contents
information by means of the time stamps of the transport streams and the addresses on
the recording medium.

60. (Currently Amended) The information recording/reproducing apparatus
according to claim 44 53 wherein, as access positions described in the management
information, positions where random accesses are possible for the contents information
are extracted.

61. (Currently Amended) The information recording/reproducing apparatus
according to claim 44 60 wherein, the contents information is inputted in the form of
transport streams prescribed by the MPEG 2 systems; and wherein

for the access positions described in the management information, transport
packets each containing a sequence header code are extracted.

62. (Canceled)

63. (Currently Amended) The information recording method according to claim 16 further comprising the steps of:

receiving enciphered contents information and ~~cipher keys~~ a contents key used to encipher the contents information ~~transmitted from other methods using communication means;~~

deciphering the contents information using the contents key;

enciphering the contents key using a medium key;

~~creating enciphered cipher keys obtained by enciphering the received cipher keys by means of the first cipher key;~~

~~deciphering the received enciphered contents information using the received cipher keys to restore contents information; and~~

recording the ~~enciphered cipher keys~~ contents key on the recording medium as the information for enciphering the contents information.

64. (Currently Amended) The information recording method according to claim 63 46 further comprising the step of:

choosing the ~~first cipher~~ medium key using a formula that includes ~~used to~~ encipher the ~~cipher keys~~ using the recording medium identification information read from the recording medium.

65. (Currently Amended) The information recording method according to claim 63 46 further comprising the steps of:

choosing the ~~first cipher~~ medium key used to encipher the contents key ~~cipher keys;~~ and

choosing ~~the second cipher~~ a master key used to encipher the medium first-cipher key using a formula that includes the recording medium identification information read ~~by~~ from the recording medium.

66. (Currently Amended) The information recording method according to claim 16 33 further comprising the steps of:

choosing ~~the second cipher~~ a master key used to encipher the medium first-cipher key ~~enciphered and read from the recording medium based on the~~ using a formula including recording medium identification information read from the recording medium;

deciphering the ~~first cipher~~ medium key enciphered by the master key ~~means of the created second cipher key~~; and

enciphering the contents key ~~received cipher keys~~ using the first-cipher medium key.

67. (Currently Amended) The information recording/reproducing method according to claim 16 further comprising the steps of:

receiving enciphered contents information and ~~cipher keys~~ a contents key used to encipher the contents information ~~transmitted from other methods using communication means~~;

creating ~~cipher key creating~~ contents key generation information that can be used to generate the contents key ~~for creating these cipher keys based on the received cipher keys~~;

~~creating enciphered cipher key creating~~ enciphering the contents key generation
with a medium key ~~information obtained by enciphering by the first cipher key the~~
~~created cipher key creating information;~~

deciphering the ~~enciphered~~ contents information received using the contents key
~~cipher keys received to restore contents information;~~ and

recording the enciphered ~~cipher key creating~~ contents key generation information
on the recording medium as the information for enciphering the contents information.

68. (Currently Amended) The information recording method according to claim 46
63 wherein, the management information shows the access positions for contents
information by means of the time information for contents information and addresses on
the recording medium.

69. (Currently Amended) The information recording method according to claim 46
68 wherein, the contents information is inputted in the form of transport streams
prescribed by the MPEG 2 systems; and wherein

the management information shows the access positions for the contents
information by means of the time stamps of the transport packets and addresses on the
recording medium.

70. (Currently Amended) The information recording method according to claim 46
63 wherein, as access positions described in the management information, positions
where random accesses are possible for the contents information are extracted.

71. (Currently Amended) The information recording method according to claim 46
70 wherein, the contents information is inputted in the form of transport packets
prescribed by the MPEG 2 systems; and wherein

for the access positions described in the management information, transport packets each containing a sequence header code are extracted.

72. (Canceled)

73. (Currently Amended) The information reproducing method according to claim 21 wherein, the recording medium contains an enciphered cipher keys contents key ~~obtained by enciphering cipher keys~~ used to encipher contents information; and further comprising the step of:

deciphering the enciphered contents key ~~cipher keys~~ by the first cipher a medium key.

74. (Currently Amended) The information reproducing method according to claim 24 73 further comprising the step of:

choosing the first cipher medium key used to decipher the contents key ~~cipher keys by means of the~~ using a formula that includes recording medium identification information read from the recording medium.

75. (Currently Amended) The information reproducing method according to claim 24 73 further comprising the steps of:

deciphering the first cipher medium key with a master key ~~used to decipher the cipher keys by means of the second cipher key~~; and

choosing the second cipher master key ~~used to decipher the first cipher key by means of the~~ using a formula that includes recording medium identification information read from the recording medium.

76. (Currently Amended) The information reproducing method according to claim 24 73 further comprising the steps of:

choosing the a master ~~second cipher~~ key for deciphering the ~~enciphered first~~
~~cipher~~ medium key read from the recording medium, the master key chosen using a
formula that includes ~~based on the~~ recording medium identification information read
from the recording medium; and

deciphering the enciphered medium ~~first cipher~~ key by means of the ~~created~~
~~second cipher~~ using the master key.

77. (Currently Amended) The information reproducing method according to claim
21 wherein[[,]] the recording medium contains enciphered contents key generation
~~enciphered cipher key creating information, the contents key generation information~~
corresponding to a contents key used to encipher the contents information ~~obtained by~~
~~enciphering cipher key creating information for creating cipher keys used to encipher~~
~~the contents information~~; further comprising the steps of:

deciphering the ~~enciphered cipher key creating~~ contents key generation
information using a medium key by means of the ~~first cipher~~ key; and

~~creating the cipher keys~~ generating the contents key based on the ~~cipher key~~
~~creating~~ contents key generation information ~~deciphered by means of the first cipher~~
key.

78. (Currently Amended) The information reproducing method according to claim
24 73 wherein, the management information shows the access positions for contents
information by means of the time information for contents information and addressed on
the recording medium.

79. (Currently Amended) The information reproducing method according to claim 24 78 wherein, the contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

the management information shows the access positions for the contents information by means of the time stamps of the transport streams and addresses on the recording medium.

80. (Currently Amended) The information reproducing method according to claim 24 73 wherein, as access positions described in the management information, positions where random accesses are possible for the contents information are extracted.

81. (Currently Amended) The information reproducing method according to claim 24 80 wherein, the contents information is inputted in the form of transport streams prescribed by the MPEG 2 systems; and wherein

for the access positions described in the management information, transport packets each containing a sequence header code are extracted.

82. (Canceled)

83. (Currently Amended) An information recording/reproducing method according to claim 26 further comprising the steps of:

during the recording process: [[.]]

receiving enciphered contents information and a contents key cipher keys used to encipher the contents information ~~transmitted from other methods by communication means,~~

deciphering the contents information using the contents key;

enciphering the contents key using a medium key;

~~creating enciphered cipher keys obtained by enciphering received cipher keys by means of the first cipher key,~~

~~deciphering the enciphered contents information received by means of the received cipher keys to restore contents information; and~~

recording the ~~enciphered cipher keys~~ contents key are recorded on the recording medium as the information for enciphering the contents information; and

during the reproducing process: [[,]]

deciphering the enciphered contents key using the medium key ~~cipher keys by means of the first cipher key.~~

84. (Currently Amended) An information recording/reproducing method according to claim 26 83 further comprising the step of:

choosing the first cipher medium key using a formula that includes ~~used to encipher the cipher keys by means of the~~ recording medium identification information read from the recording medium.

85. (Currently Amended) An information recording/reproducing method according to claim 26 83 further comprising the steps of:

choosing the first cipher medium key used to encipher the contents key cipher keys; and

choosing the second cipher a master key used to encipher the first cipher medium key ~~by means of the~~ using a formula that includes recording medium identification information read from the recording medium.

86. (Currently Amended) An information recording/reproducing method according to claim 26 83 further comprising the steps of:

choosing ~~the second cipher~~ a master key for deciphering the medium first-
enciphered cipher key read from the recording medium, using a formula including based
on the recording medium identification information read from the recording medium; and
deciphering the first enciphered cipher medium key by means of the second-
cipher using the master key created; and

wherein the cipher keys received contents key is are deciphered using the
medium key by means of the first cipher key.

87. (Currently Amended) An information recording/reproducing method according
to claim 26 further comprising the steps of:

during the recording process: [[,]]

receiving enciphered contents information and a contents key cipher keys used
to encipher the contents information ~~transmitted from other methods by communication-~~
means,

creating ~~cipher key creating~~ contents key generation information that can be
used to generate the contents key for creating these cipher keys based on the cipher-
keys received,

~~creating enciphered cipher key creating~~ enciphering the contents key generation
information with a medium key information obtained by enciphering the created cipher-
key creating information by means of the first cipher key,

deciphering the received enciphered contents information using the contents key
received by means of the cipher keys received to restore contents information, and

recording the enciphered contents key generation ~~cipher key creating~~ information
on the recording medium as the information for enciphering the contents information;
and

during the reproducing process: [[.]]

deciphering the enciphered ~~cipher key creating~~ contents key generation
information ~~by means of the first cipher~~ using the medium key, and
creating the contents key using ~~cipher keys based on the cipher~~ contents key
~~creating generation~~ information ~~deciphered by the first cipher key~~.

88. (Currently Amended) An information recording/reproducing method according
to claim 26 83 wherein, the management information shows the access positions for
contents information by means of the time information for contents information and the
addresses on the recording medium.

89. (Currently Amended) An information recording/reproducing method according
to claim 26 88 wherein, the contents information is inputted in the form of transport
streams prescribed by the MPEG 2 systems; and wherein

the management information shows the access positions for the contents
information by means of the time stamps of the transport streams and the addresses on
the recording medium.

90. (Currently Amended) An information recording/reproducing method according
to claim 26 83 wherein, as access positions described in the management information,
positions where random accesses are possible for the contents information are
extracted.

91. (Currently Amended) An information recording/reproducing method according to claim 26 90 wherein, the contents information is inputted in the form of transport packets prescribed by the MPEG 2 systems; and wherein

for the access positions described in the management information, transport packets each containing a sequence header code are extracted.

92. (Currently Amended) A recording medium wherein the following are recorded:

enciphered contents information,
information for enciphering the contents information, and
processor readable management information that includes instructions for causing the computer processor to ~~access~~ process data at recording medium access positions on the recording medium, the recording medium access positions indicating addresses on the recording medium corresponding to a time stamp in the contents information.